

12-21-05

AFS
JGW

Express Mailing Label No.: EV 589980234 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of	Atty. Docket No.:	2391-002
Dale BURNS	Conf. No. :	9242
Appln. No.: 09/491,919	Group Art Unit:	2135
Filing Date: Jan. 27, 2000	Examiner:	Dada, Beemnet W.

For: **SYSTEM AND METHOD FOR EMAIL SCREENING**

APPEAL BRIEF TRANSMITTAL

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Enclosed, please find:

1. Appellants' Brief on Appeal in response to the Final Rejection dated May 17, 2005; and
2. A check in the amount of \$250.00 in accordance with 37 CFR 41.20(b)(2).

The Commissioner for Patents is hereby authorized to charge all necessary fees or credit any overpayments to the Deposit Account No. 18-1579. A duplicate copy of this letter is enclosed.

Respectfully submitted,

Christopher B. Kilner, Reg. No. 45,381
Roberts Abokhair & Mardula, LLC
11800 Sunrise Valley Dr., Suite 1000
Reston, VA 20191
(703) 391-2900



Express Mailing Label No.: EV 589980234 US

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

In re Application of	Atty. Docket No.:	2391-002
Dale BURNS	Conf. No. :	9242
Appln. No.: 09/491,919	Group Art Unit:	2135
Filing Date: Jan. 27, 2000	Examiner:	Dada, Beemnet W.

For: **SYSTEM AND METHOD FOR EMAIL SCREENING**

APPELLANTS' BRIEF ON APPEAL UNDER 37 C.F.R. 41.37(c)(1)

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In accordance with the provisions of 37 C.F.R. § 41.37, Appellants submits the following:

(i) *Real party in interest.*

Based on information supplied by Appellants, and to the best of Appellants' legal representatives' knowledge, the real party in interest is the inventors, Mr. Dale Burns and Mr. Theodore Palles.

(ii) *Related appeals and interferences.*

Appellants, as well as Appellants' assigns and legal representatives are unaware of any appeals or interferences which will be directly affected by, or which will directly affect, or have a bearing on the Board's decision in the pending appeal.

App. No. 09/491,919
Appeal Brief

(iii) Status of claims.

Claims 1-15 are currently pending. No claims have been allowed. No claims have been canceled. Claims 1-15 are appealed. Claims 1-15 are set forth in the Appendix.

(iv) Status of amendments.

The amendment to the claims filed May 24, 2004 was entered.

(v) Summary of claimed subject matter.

The subject matter defined in independent claim 1 is an email screening system comprising: a recipient computer connected to a network (page 7, lines 4-5 and 13-17; page 10, lines 5-10; figure 1, reference numerals 16 and 14); an email screening server connected to the recipient computer over the network (page 7, lines 8-11; page 10, lines 5-10; figure 1, reference numerals 12 and 14); a sender computer connected to the recipient computer and the email screening computer over the network (page 7, lines 12-17; page 10, lines 5-10; figure 1, reference numerals 10 and 14); wherein said recipient computer further comprises software instructions for forwarding all email messages received to the email screening server (page 5, lines 5-10; page 6, lines 8-10; page 7, lines 18-20; page 8, lines 1-3; figure 2, reference numerals 20-22); and wherein the email screening server further comprises software instructions for screening the email for viruses and notifying the sender computer that the email will be forwarded to the recipient computer for a fee (page 5, line 11 to page 6, line 4; page 6, lines 11-17; page 7, lines 20-22; page 9, line 19 to page 10, line 4; figure 2, reference numerals 24, 26, 30, 32, 34, and 28);.

The subject matter defined in independent claim 9 is a method for detecting viruses in email and administrating email for a recipient comprising: an email screening server connected to a network (page 7, lines 8-11; page 10, lines 5-10; figure 1, reference numerals 12 and 14) assigning a password (page 6, 11-13; page 11, lines 13-14) to an email recipient connected to the network (page 7, lines 4-5 and 13-17; page 10, lines 5-10; figure 1, reference numerals 16 and 14); software on a recipient computer rerouting email received by the email recipient computer to the email screening server over the network (page 5, lines 5-10; page 6, lines 8-10; page 7, lines 18-20; page 8, lines 1-3; figure 1, reference numerals 12, 16, and 14; figure 2, reference

numerals 20-22); screening the email by the email screening server for viruses (page 5, line 11; page 6, line 11; page 8, lines 3-4; figure 2, reference numeral 24); forwarding screened email to a recipient computer if the email possess a recipient password; (page 8, lines 6-11; figure 2, reference numerals 26 and 28); and holding email at the email screening server when the email is without the recipient password (page 8, line 12 to page 9, line 12; figure 2, reference numerals 40 and 38).

The subject matter defined in independent claim 10 is a method of virus screening of email comprising: a recipient computer (page 7, lines 4-5 and 13-17; page 10, lines 5-10; figure 1, reference numeral 16) re-routing received email from the recipient computer to a screening server over a network (page 5, lines 5-10; page 6, lines 8-10; page 7, lines 18-20; page 8, lines 1-3; figure 1, reference numerals 12 and 14; figure 2, reference numerals 20-22); the screening server scanning the email for a virus (page 5, line 11; page 6, line 11; page 8, lines 3-4; figure 2, reference numeral 24); the screening server notifying the sender computer of the email that the scanned email will be sent to the recipient computer for a fee (page 5, line 21 to page 6, line 1; page 9, lines 1-7; figure 2, reference numeral 30); the screening server sending the scanned email to the recipient computer over the network if the fee is paid (page 9, lines 8-12; figure 2, reference numerals 32 and 28); and sharing the fee with a recipient associated with the recipient computer (page 6, lines 1-4).

(vi) Grounds of rejection to be reviewed on appeal.

Ground 1 - Are claims 1 and 10 unpatentable under 35 USC 103 as being obvious over Council in view of Hypponen et al.?

Ground 2 - Are claims 2-9 and 11-15 unpatentable under 35 USC 103 as being obvious over Council and Hypponen et al. as applied to claims 1 and 10 and further in view of Hardy et al.?

(vii) Argument.

Background

In response to prior rejections of the claims based upon obviousness in view of Council, Ji et al., and/or Hardy et al., Appellants previously submitted that neither Council, Ji et al., nor Hardy et al. disclose or fairly suggest *forwarding or re-routing* from the *recipient computer* to a

screening server. Appellants' representative and the Examiner agreed that the reference to Ji et al. was relied upon in all the rejections for the virus-scanning limitations. Appellants' representative and the Examiner further agreed that Ji et al. teaches scanning *at the client node* (recipient computer). See, e.g., the abstract and figures 11a-11c and the related text in columns 15-16.

Applicants' representative discussed the following with respect to the claim limitations:

- Claim 1 includes "*wherein said recipient computer further comprises software instructions for forwarding all email messages received to the email screening server;*"
- Claim 6 includes "*software on a recipient computer rerouting email received by the email recipient computer to the email screening server over the network;*" and
- Claim 10 includes "*a recipient computer re-routing received email from the recipient computer to a screening server over a network.*"

Appellants' representative then submitted that the prior art failed to teach or fairly suggest forwarding or re-routing of e-mail messages received at a recipient computer to a screening server. The prior art teaches scanning at ISP-level (e.g., BrightMail) or at the firewall/gateway server prior to delivery to a recipient computer or scanning at a recipient computer (e.g., Norton anti-virus). The ordinary path of e-mail delivery is followed. In the present invention, the path is extended by having *all the e-mail sent back out to a screening server* before any ultimate delivery back to the recipient. As such, a user is not limited to what ISP they use and is not required to make updates to any local virus screening software.

In response, the Examiner and Appellants' representative agreed that the Ji et al. patent failed to teach or fairly suggest forwarding or re-routing of e-mail messages received at a recipient computer to a screening server such that the rejections in the Office Action mailed October 7, 2004 failed to make a *prima facie* case of obviousness and that further search and consideration by the Examiner was required. This was documented in Appellants' Reply under 37 CFR 1.111 filed February 7, 2005 and the Interview Summary included in the Office Action of May 17, 2005.

The final rejection, mailed May 17, 2005 and presently appealed, apparently substitutes the published application of Hypponen et al. for the Ji et al. reference, but suffers from essentially the same problems previously discussed with the Examiner regarding Ji et al., as submitted below.

Grounds 1 - Rejection of Claims 1 and 10 under 35 USC 103

Claims 1 and 10 were rejected under 35 USC 103 as being obvious over Council in view of Hypponen et al.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. (See M.P.E.P. Section 2143). In the present case, there is no proper motivation to combine the references and the prior art references, even when combined, fail to teach or suggest all the claim limitations.

Claim 1

The Office Action fails to provide a proper motivation to combine Council with Hypponen et al. Page 3, lines 3-5 of the Office Action state the motivation as “It would have been obvious to one having ordinary skill in the art at the time of applicant’s invention to modify the teachings of Hypponen within the system of Council, in order to further allow centralized email screening by forwarding received email to a screening system and further enhance the security of the system.” As such, the ostensible reasons to combine the references are centralization and security.

However, Council already teaches centralized email screening by email address at an ISP (see Col. 2:33-47), and thus has no reason to look to any teachings of Hypponen et al. regarding centralized screening. Council also fails to make any suggestion regarding security because it is concerned with email *authorization*, not with email *security*, and therefore has no reason to look to any other source for additional security.

Hypponen et al. teaches interception of suspect emails and centralized screening. It has nothing to do with authorizations lists or the billing of email-sending parties (the objects of Council). It is unclear why anyone would seek to combine its teachings with Council absent a hindsight attempt to reconstruct Appellants’ claims.

The more likely result of a combination of Council with Hypponen et al. would be an email screening system in which multiple ISP (transit nodes) looked to a central server for an updated authorization list.

Even if it were proper to combine Council with Hypponen et al., the combination fails to teach or suggest all the claim limitations. As previously presented with respect to Ji et al., Hypponen et al. also fails to teach or fairly suggest a “recipient computer” with “software instructions for forwarding all email messages received to the email screening server,” such that the rejection of claim 1 in the Office Action mailed May 17, 2005 fails to make a *prima facie* case of obviousness.

While Hypponen et al. admittedly does not teach scanning at the recipient computer (a previous issue with Ji et al.), Hypponen et al. still ascribes to the prior art method of virus scanning by *interception* at a firewall/gateway *prior to ever being delivered to a recipient computer* (see paragraphs [0011] to [0014] and the first box of figure 2). Although Hypponen et al. suggests the re-routing of certain types of data to a screening server (see paragraph [0035]), it still relies on a few “protected systems” to intercept and re-route the mail, and thus the system will only work when a user is attached to the network with the “protected systems.” In the present invention, the recipient computer can be connected to any network, not just a protected one.

Further, in the system of Hypponen et al., only certain types of data are intercepted and scanned (see paragraph [0035] and figure 2). Likewise, it is inherent that the agents on the protected systems must be updated to determine what is currently “suspect data” for the system to work since, as stated in paragraph [0036], “Data which is not of a suspect type is passed over by the agent and is routed by the system to its intended user 2.” As such, not all mail is sent to a scanning server. The present invention of claim 1, however, re-routes *all* mail received by the recipient computer such that the only machine that needs up-to-date software is the screening server (see “said recipient computer further comprises software instructions for forwarding *all* email messages received to the email screening server” of claim 1).

As previously submitted to the Patent Office, the prior art of: Council teaches screening of unwelcome or unsolicited email messages (which may contain a virus) based upon *delivering mail only if the sender is on an authorized list*; Hypponen et al. discloses a method of detecting viruses in a computer network comprising *intercepting* data at at least one data *transit node* of

the network. The transit nodes that employ the invention are called “protected systems” which are described in paragraph [0032] as “firewall 4a, mail server 4b, a proxy server 4c and a database server 4d.” These protected systems are not *recipient computers* (called “users or clients 2” in paragraph [0031]), but rather *transit computers*, and they identify which of the network data is of a type capable of containing a virus and transfers the identified data to a virus scanning server 7 over the network. In use, an email recipient is only protected when accessing email over the network that has the protected systems; Ji et al. teaches virus scanning *at the client node* (recipient computer). See, e.g., the abstract and figures 11a-11c and the related text in columns 15-16; Hardy et al. teaches *password-based authorization* and has no teachings regarding virus screening; Kim et al. teaches virus scanning, sniffing, or detecting of e-mail viruses *prior to the e-mail messages arriving at the destination system* or server; Aronson et al. teaches a server for filtering e-mail messages wherein the server receives requests to retrieve e-mail messages on behalf of a client and then retrieves e-mail messages from a mail server on behalf of the client. The *server then filters* the e-mail messages based on one or more rules and transfers the filtered e-mail messages to the client; Franczek et al. teaches the screening of computer data for viruses within a telephone network *before communicating the computer data to an end user*; Tso et al. teaches a system for virus checking a data object to be downloaded to a client device that is implemented in a method including the steps of retrieving a data object to be downloaded, scanning the data object for a computer virus, and *downloading the data object to the client device if no computer virus is detected*; Dickenson et al. teaches an *e-mail firewall* that applies policies to e-mail messages between a first site and a plurality of second sites in accordance with a plurality of administrator selectable policies; and Chen et al. teaches a message system, *located at the server computer, that controls the distribution of e-mail messages*, wherein an anti-virus module, *located at the server computer*, scans files for viruses.

None of these prior art systems include *recipient computer software* to re-route or forward received email to a scanning server. The prior art is primarily drawn to interception and scanning/cleaning of email at intermediate points in the delivery process. Hypponen et al. continues to teach this sort of system based upon interception by “protected systems” prior to suspect data being delivered to a user on the network with the protected systems.

For the above-cited reasons, Appellants submit that the Office Action has failed to establish a *prima facie* case of obviousness for claim 1.

Claim 10

As with claim 1, there is no proper motivation to combine Council with Hypponen et al. Council already teaches centralized email screening by email address at an ISP (see Col. 2:33-47), and thus has no reason to look to any teachings of Hypponen et al. regarding centralized screening. Council also fails to make any suggestion regarding security because it is concerned with email *authorization*, not with email *security*, and therefore has no reason to look to any other source for additional security.

Hypponen et al. teaches interception of suspect emails and centralized screening. It has nothing to do with authorizations lists or the billing of email-sending parties (the objects of Council). It is unclear why anyone would seek to combine its teachings with Council absent a hindsight attempt to reconstruct Appellants' claims.

The combination of Council with Hypponen et al. also fails to teach or fairly suggest "a recipient computer re-routing received email from the recipient computer to a screening server over a network" as required by claim 10 such that the rejection of claim 10 in the Office Action mailed May 17, 2005 fails to make a *prima facie* case of obviousness.

Hypponen et al. ascribes to the prior art method of virus scanning by *interception* at a firewall/gateway *prior to ever being delivered to a recipient computer* (see paragraphs [0011] to [0014] and the first box of figure 2). Although Hypponen et al. suggests the re-routing of certain types of data to a screening server (see paragraph [0035]), it still relies on a few "protected systems" to intercept and re-route the mail, and thus the system will only work when a user is attached to the network with the "protected systems." In the present invention, the recipient computer can be connected to any network, not just a protected one.

For the above-cited reasons, Appellants submit that the Office Action has failed to establish a *prima facie* case of obviousness for claim 10.

Grounds 2 - Rejection of Claims 2-9 and 11-15 under 35 USC 103

Claims 2-9 and 11-15 were rejected under 35 USC 103 as being obvious over Council and Hypponen et al. as applied to claims 1 and 10 and further in view of Hardy et al.

Claims 2-9

Claims 2-9 are allowable for the same reasons identified above with respect to claim 1 since the base combination of Council and Hypponen et al. failed to establish a *prima facie* case

of obviousness. The addition of Hardy et al. fails to cure any of the defects of the base combination.

Hardy et al. discloses a key or authority server. Hardy et al., like Council and Hypponen et al., fails to teach or fairly suggest a “recipient computer” with “software instructions for forwarding all email messages received to the email screening server” as required by claim 1 such that the rejection in the Office Action mailed May 17, 2005 fails to make a *prima facie* case of obviousness.

With regard to the propriety of combining Hardy et al. with Council and Hypponen et al., Appellants submit that the Office Action motivational statement “because such [authorization] list[s] are difficult to keep up” lacks any basis or foundation in the prior art. As per MPEP 2143.01, “There are three possible sources for a motivation to combine references: the nature of the problem to be solved, the teachings of the prior art, and the knowledge of persons of ordinary skill in the art.” *In re Rouffet*, 149 F.3d 1350, 1357, 47 USPQ2d 1453, 1457-58 (Fed. Cir. 1998) (The combination of the references taught every element of the claimed invention, however without a motivation to combine, a rejection based on a *prima facie* case of obvious was held improper.)

Appellants further submit that an authorization list for email delivery (e.g., a “whitelist”) of Council is quite different (and arguably non-analogous) from authorization keys and signatures used for encryption and verification, as taught by Hardy et al.

Neither Council nor Hypponen et al. suggest any desirability of or need for authorization keys and signatures used for encryption and verification, as taught by Hardy et al., and Hardy et al. fails to suggest the application of keys, signatures, or passwords to email screening. As such, Appellants submit that the Office Action rejection has used impermissible hindsight to combine the references.

For the above-cited reasons, Appellants submit that the Office Action has failed to establish a *prima facie* case of obviousness for claims 2-9.

Claim 3

The Office Action alleges that “software instructions for holding all email messages without the password” is inherent in a system that is not authorized to send mail. Appellants submit that this is a logical fallacy. Holding email is not inherent in not sending it since other

options such as deleting or sending to another location exist. Council, which deals with the authorization issue, teaches informing the sending party at 23 of figure 2, yet explicitly mentions saving in other boxes 18 and 21. Hypponen et al. deals with a different matter of viruses and teaches quarantining data and informing an administrator, which is different than “holding” an email.

For the above-cited reason, Appellants submit that the Office Action has failed to establish a *prima facie* case of obviousness for claim 3.

Claim 8

The Office Action alleges that “providing the recipient computer with the option to receive the email without the recipient password” is obvious without any supporting evidence beyond an “obvious to try” rationale related to “if the recipient is out of town...” that is improper under MPEP 2143.01 since the “mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990) (Claims were directed to an apparatus for producing an aerated cementitious composition by drawing air into the cementitious composition by driving the output pump at a capacity greater than the feed rate. The prior art reference taught that the feed means can be run at a variable speed, however the court found that this does not require that the output pump be run at the claimed speed so that air is drawn into the mixing chamber and is entrained in the ingredients during operation. Although a prior art device “may be capable of being modified to run the way the apparatus is claimed, there must be a suggestion or motivation in the reference to do so.” 916 F.2d at 682, 16 USPQ2d at 1432.). See also *In re Fritch*, 972 F.2d 1260, 23 USPQ2d 1780 (Fed. Cir. 1992) (flexible landscape edging device which is conformable to a ground surface of varying slope not suggested by combination of prior art references).”

Council, which deals with the authorization issue, teaches informing the sending party at 23 of figure 2, yet explicitly mentions saving in other boxes 18 and 21. Hypponen et al. deals with a different matter of viruses and teaches quarantining data and informing an administrator, which is different than “holding” an email that lacks a password.

For the above-cited reason, Appellants submit that the Office Action has failed to establish a *prima facie* case of obviousness for claim 8.

Claims 11-15

Claims 11-15 are allowable for the same reasons identified above with respect to claim 10 since the base combination of Council and Hypponen et al. failed to establish a *prima facie* case of obviousness. The addition of Hardy et al. fails to cure any of the defects of the base combination.

Hardy et al. discloses a key or authority server. Hardy et al., like Council and Hypponen et al., fails to teach or fairly suggest “a recipient computer re-routing received email from the recipient computer to a screening server over a network” as required by claim 10 such that the rejection of claim 10 in the Office Action mailed May 17, 2005 fails to make a *prima facie* case of obviousness.

With regard to the propriety of combining Hardy et al. with Council and Hypponen et al., Appellants submit that an authorization *list* for email delivery (e.g., a “whitelist”) of Council is quite different from authorization *keys* and *signatures* used for encryption and verification, as taught by Hardy et al.

As per MPEP 2143.01, “There are three possible sources for a motivation to combine references: the nature of the problem to be solved, the teachings of the prior art, and the knowledge of persons of ordinary skill in the art.” *In re Rouffet*, 149 F.3d 1350, 1357, 47 USPQ2d 1453, 1457-58 (Fed. Cir. 1998) (The combination of the references taught every element of the claimed invention, however without a motivation to combine, a rejection based on a *prima facie* case of obvious was held improper.)

Neither Council nor Hypponen et al. suggest any desirability of or need for authorization keys and signatures used for encryption and verification, as taught by Hardy et al., and Hardy et al. does not suggest the application of its disclosed keys, signatures, or passwords *to email screening*. The Office Action motivational statement “because such [authorization] list[s] are difficult to keep up” lacks any basis or foundation in the prior art. As such, Appellants submit that the Office Action rejection has used impermissible hindsight to combine the references.

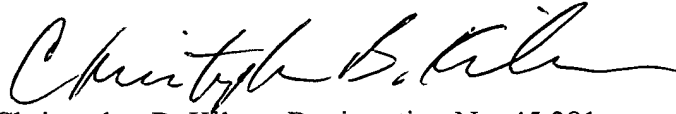
For the above-cited reasons, Appellants submit that the Office Action has failed to establish a *prima facie* case of obviousness for claims 11-15.

Conclusion

For the above reasons, Appellants respectfully submit that the present claims meet the requirements of 35 U.S.C. 102 and 103 and that the Examiner has failed to make out a *prima facie* case of obviousness, and asks that the rejections be reversed.

Respectfully submitted,

ROBERTS ABOKHAIR & MARDULA, LLC

A handwritten signature in black ink, appearing to read "Christopher B. Kilner". The signature is fluid and cursive, with a long horizontal stroke at the end.

Christopher B. Kilner, Registration No. 45,381
Roberts Abokhair & Mardula, LLC
11800 Sunrise Valley Drive, Suite 1000
Reston, VA 20191-5302
(703) 391-2900

(viii) Claims appendix.

1. An email screening system comprising:
 - a recipient computer connected to a network;
 - an email screening server connected to the recipient computer over the network;
 - a sender computer connected to the recipient computer and the email screening computer over the network;wherein said recipient computer further comprises software instructions for forwarding all email messages received to the email screening server; and
 - wherein the email screening server further comprises software instructions for screening the email for viruses and notifying the sender computer that the email will be forwarded to the recipient computer for a fee.
2. The email screening system of claim 1 wherein the recipient computer further comprises a password assigned to the recipient computer by the email screening computer.
3. The email screening system of claim 2 wherein the instructions stored by said email screening server further comprise software instructions for holding all email messages without the password.
4. The email screening system of claim 2 wherein the email screening server further comprises software instructions for alerting the recipient computer that an email message without the password is being held by the email screening computer.
5. The email screening system of claim 4 wherein the software instructions stored by the email screening server further comprise software instructions for charging the sender associated with a sender computer a fee to forward said email message without the password to the recipient computer.
6. A method for detecting viruses in email and administrating email for a recipient comprising:

an email screening server connected to a network assigning a password to an email recipient connected to the network;

software on a recipient computer rerouting email received by the email recipient computer to the email screening server over the network;

screening the email by the email screening server for viruses;

forwarding screened email to a recipient computer if the email possess a recipient password; and

holding email at the email screening server when the email is without the recipient password.

7. The method of claim 6 further comprising:

notifying the recipient computer that the email without the recipient password is being held;

notifying a sender computer that the email without the recipient password is being held; and

charging a sender associated with the sender computer a fee for sending the email without the recipient password.

8. The method of claim 7 further comprising:

providing the recipient computer with the option to receive the email without the recipient password.

9. The method of claim 7 further comprising sharing the fee charged to the sender with the recipient associated with the recipient computer when the recipient computer accepts the email without the recipient password.

10. A method of virus screening of email comprising:

a recipient computer re-routing received email from the recipient computer to a screening server over a network;

the screening server scanning the email for a virus;

the screening server notifying the sender computer of the email that the scanned email will be sent to the recipient computer for a fee;

the screening server sending the scanned email to the recipient computer over the network if the fee is paid; and

sharing the fee with a recipient associated with the recipient computer.

11. The method of virus screening of email of claim 10 further comprising:

the screening server establishing a password for the recipient;

the recipient notifying selected email senders of the password;

the screening server scanning the email for the password;

the screening server forwarding the email from the selected senders when the email possesses the password; and

the screening server making no charge to the selected e-mail sender.

12. The method of claim 10 further comprising automatically forwarding email when said email message has an identification password.

13. The method of claim 10 further comprising:

sending a notification message to said sender computer when an identification password is not detected; and

charging a sender associated with the sending computer a fee to send said email to said recipient computer.

14. The method of claim 13 further comprising:

sharing a portion of said fee with said recipient.

15. The method of claim 10 further comprising:

sending a notification message to said sender computer and said recipient computer when an identification password is not detected; and

providing a recipient with an option to pay for screening and sending said email when said sender does not pay for screening and sending said email.

(ix) *Evidence appendix.*

No evidence was submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 and no other evidence was entered by the examiner and relied upon by appellant in the appeal.

(x) *Related proceedings appendix.*

There are no related proceedings.